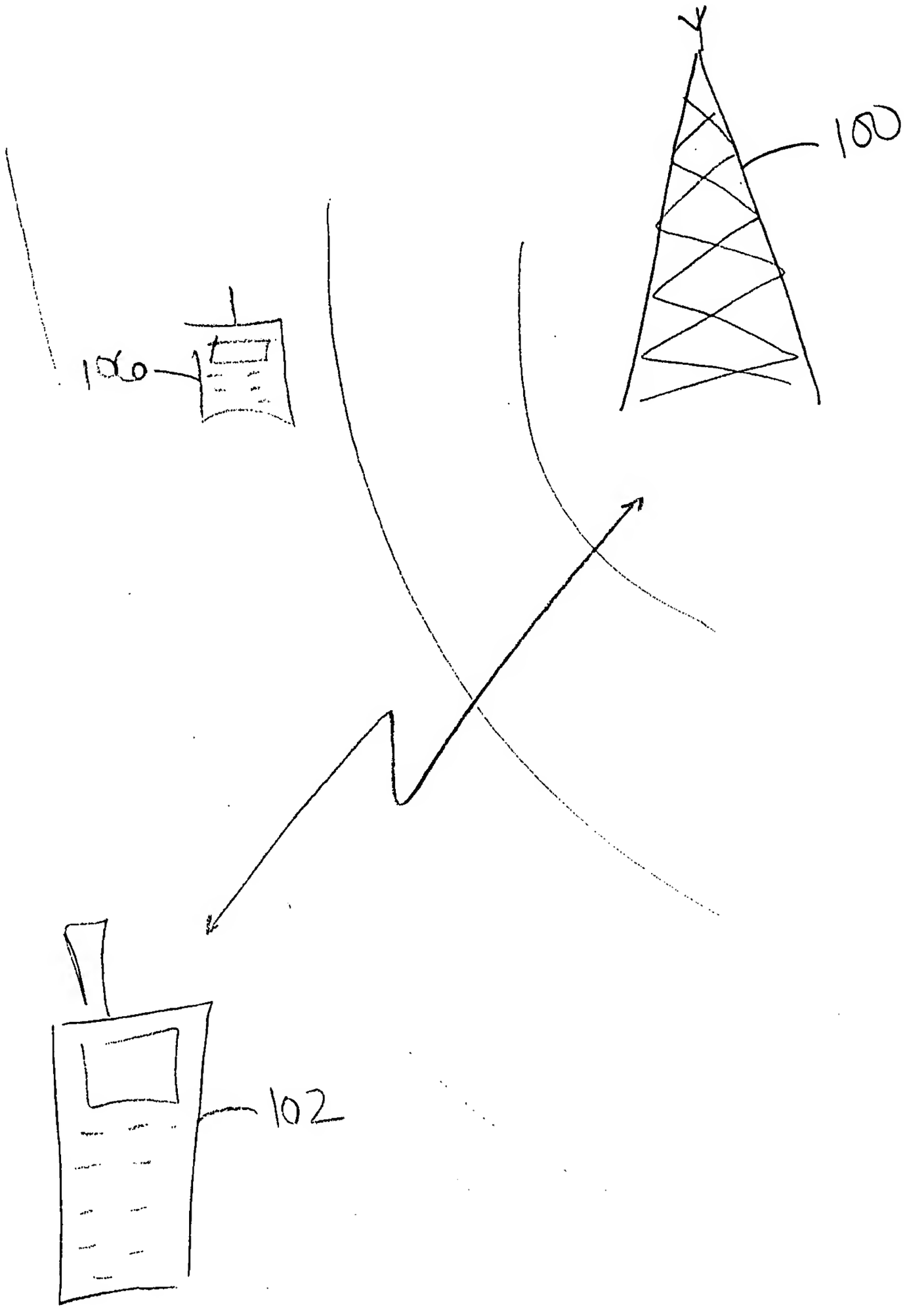
CM06214H
Silverman et al

FIG. 1

1/7



200

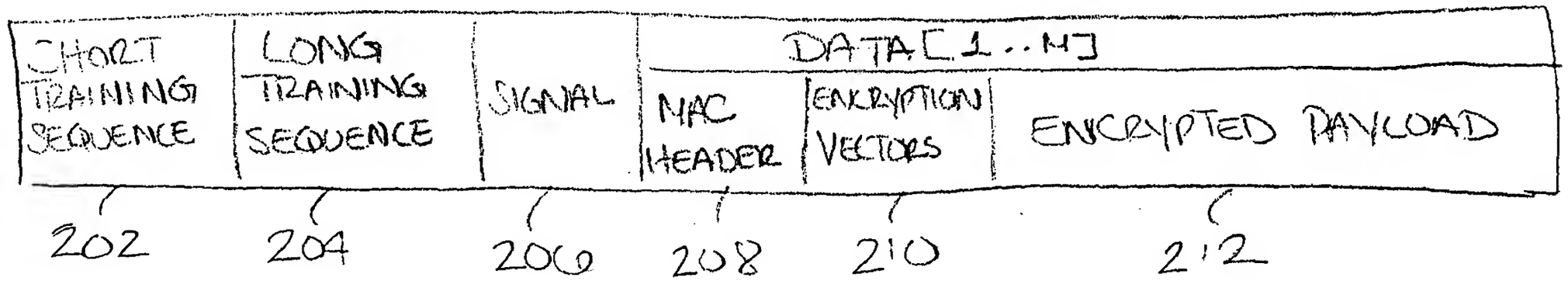


FIG. 2

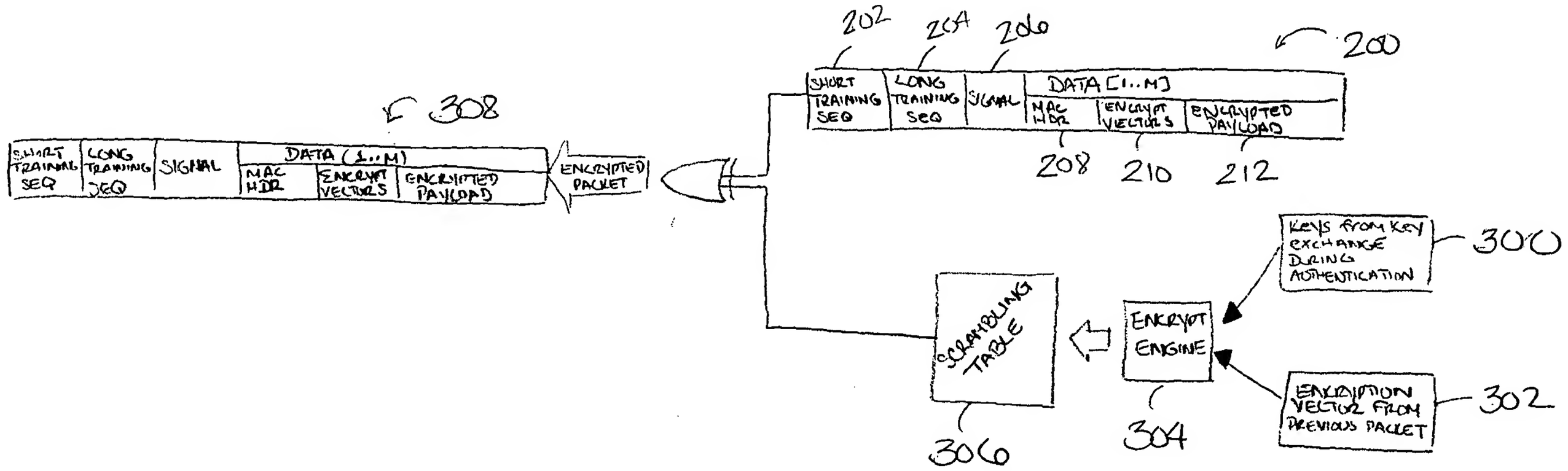


FIG. 3

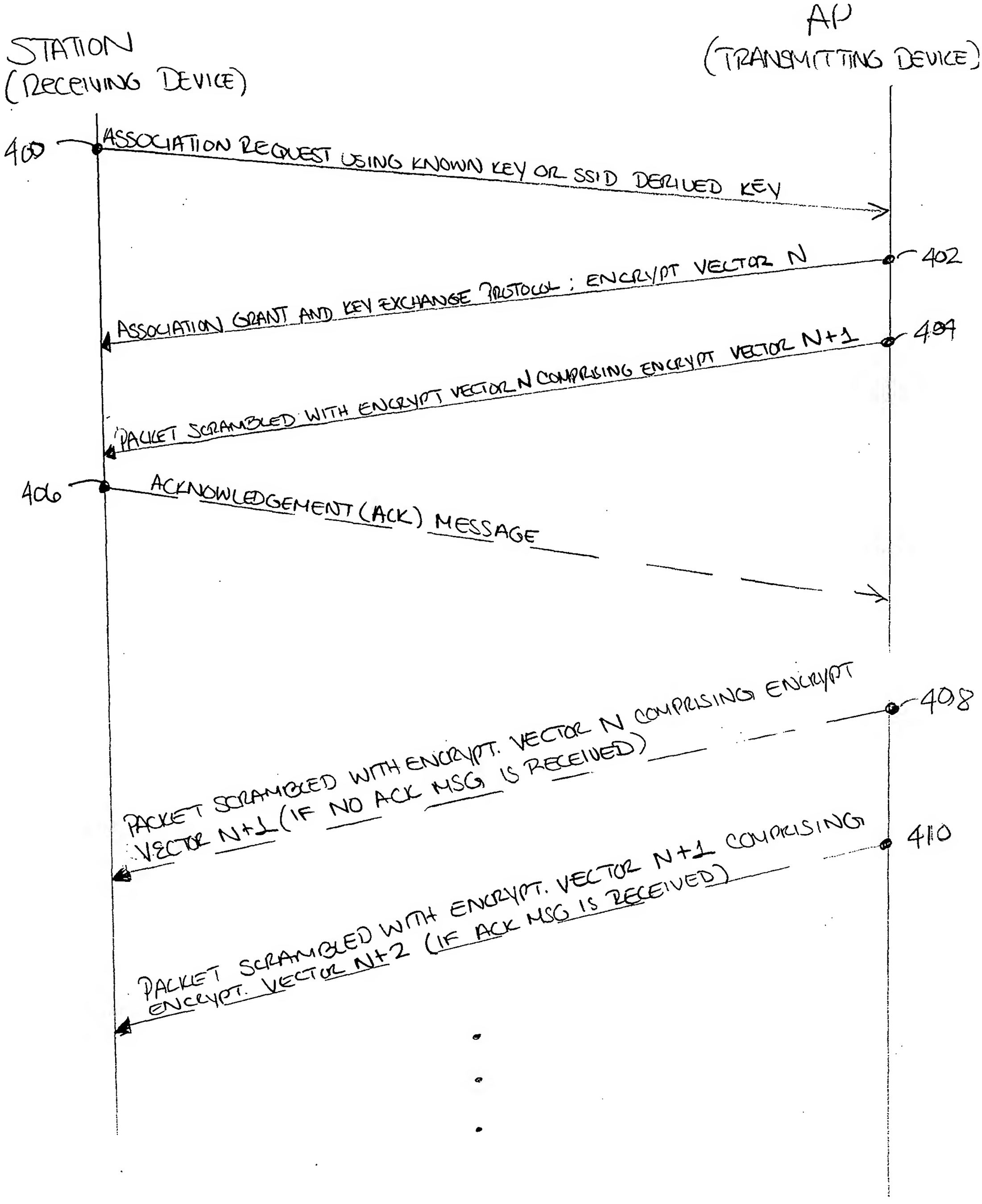

STATION
(RECEIVING DEVICE)
AP
(TRANSMITTING DEVICE)
400
ASSOCIATION REQUEST USING KNOWN KEY OR SSID DERIVED KEY
402
ASSOCIATION GRANT AND KEY EXCHANGE PROTOCOL ; ENCRYPT VECTOR N
404
PACKET SCRAMBLED WITH ENCRYPT VECTOR N COMPRISING ENCRYPT VECTOR N+1
406
ACKNOWLEDGEMENT (ACK) MESSAGE
408
PACKET SCRAMBLED WITH ENCRYPT. VECTOR N COMPRISING ENCRYPT VECTOR N+1 (IF NO ACK MSG IS RECEIVED)
410
PACKET SCRAMBLED WITH ENCRYPT. VECTOR N+1 COMPRISING ENCRYPT. VECTOR N+2 (IF ACK MSG IS RECEIVED)

FIG. 4

FIG 5

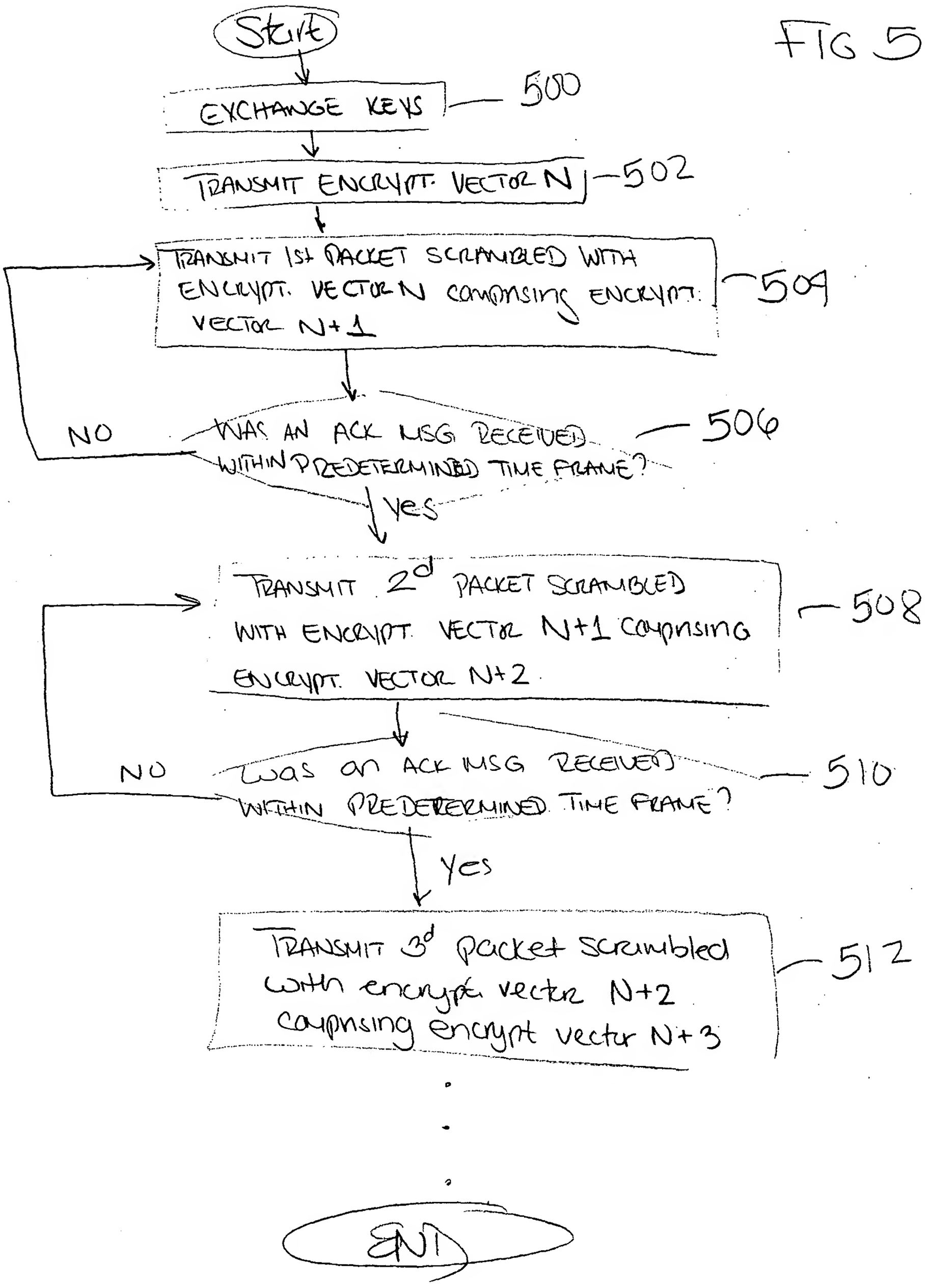

Start
EXCHANGE KEYS
500
TRANSMIT ENCRYPT. VECTOR N
502
TRANSMIT 1st PACKET SCRAMBLED WITH ENCRYPT. VECTOR N COMPRISING ENCRYPT. VECTOR N+1
504
NO
WAS AN ACK MSG RECEIVED WITHIN PREDETERMINED TIME FRAME?
506
YES
TRANSMIT 2d PACKET SCRAMBLED WITH ENCRYPT. VECTOR N+1 COMPRISING ENCRYPT. VECTOR N+2
508
NO
WAS AN ACK MSG RECEIVED WITHIN PREDETERMINED TIME FRAME?
510
YES
TRANSMIT 3d Packet Scrambled with encrypt vector N+2 comprising encrypt vector N+3
512
END

FIG. 6
5/7

START

EXCHANGE KEYS — 600

RECEIVE ENCRYPT. VECTOR N — 602

RECEIVE a PACKET — 604

Decrypt at least a portion of the packet using encrypt. vector N — 606

TRANSMIT ACK MSG for the packet — 608

Receive a packet — 610

Attempt to decrypt at least a portion of the packet using encrypt. vector N and encrypt vector N+1 — 612

was encrypt. vector N successful in decrypting at least the portion of the packet? — 614

Yes

NO

WAIT UNTIL Receipt of entire packet — 616

TRANSMIT ACK MSG for the packet — 618

Receive a packet — 620

Attempt to decrypt at least a portion of the packet using encrypt. vector N+1 and encrypt. vector N+2 — 622

was encrypt. vector N+1 successful in decrypting at least a portion of the packet? — 624

Yes

NO

Wait until receipt of entire packet — 626

TRANSMIT ACK MSG for the packet — 628

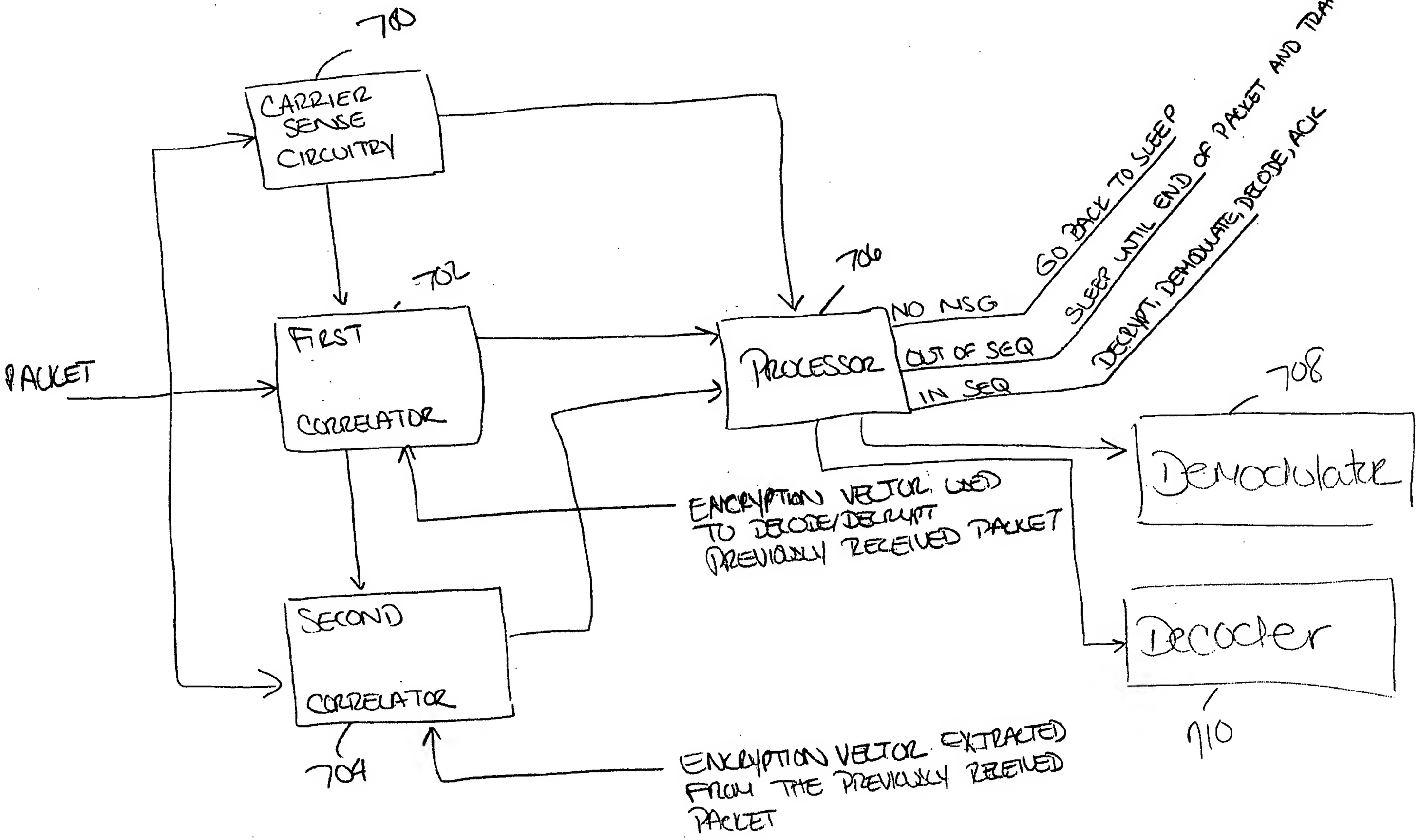

700
CARRIER SENSE CIRCUITRY
702
FIRST CORRELATOR
PACKET
706
PROCESSOR
NO NSG
GO BACK TO SLEEP
OUT OF SEQ
SLEEP UNTIL END OF PACKET AND TRANSMIT ACK MSG
IN SEQ
DECRYPT, DEMODULATE, DECODE, ACK
708
DEMODULATOR
ENCRYPTION VECTOR USED TO DECODE/DECRYPT PREVIOUSLY RECEIVED PACKET
DECODER
710
SECOND CORRELATOR
704
ENCRYPTION VECTOR EXTRACTED FROM THE PREVIOUSLY RECEIVED PACKET

FIG. 7

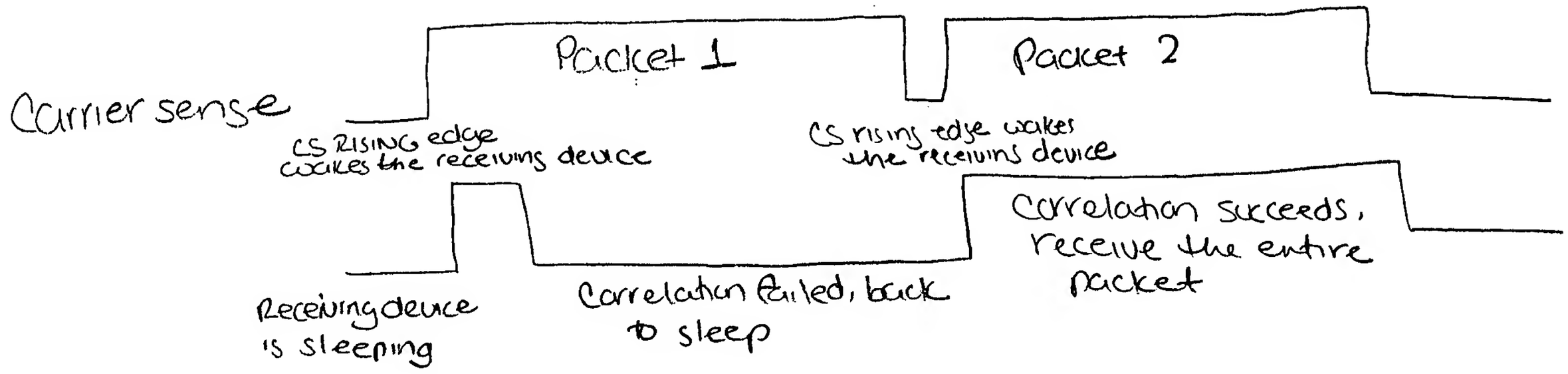

Carrier sense
Packet 1
Packet 2
CS RISING edge wakes the receiving device
CS rising edge wakes the receiving device
Receiving device is sleeping
Correlation failed, back to sleep
Correlation succeeds, receive the entire packet

FIG. 8

9/n